

2 / P
422 Rec'd PCT/PTO 24 AUG 2000

1

INSA17

METHOD AND DEVICE FOR SECURING ACCESS TO A SERVICE IN A TELECOMMUNICATION NETWORK

The invention relates to a method for accessing a service in a telecommunication network, ^{which may be} ~~be it~~ a private network, an intelligent network or a mobile radio network ^{a2} ~~proceeding~~ from an arbitrary communication terminal device, ^{a3} ~~wherein it is necessary~~ to authenticate oneself by means of entering digit sequences in order to receive access to a desired service. ^{in addition} ~~Besides~~, the invention relates to a device in a telecommunication network, which makes it possible to carry out a secure authentication of a user in the case of a service call.

Description of the Related Art

Given an intelligent network IN, an architecture is concerned that makes it possible, in a communication network, to offer services to users of this network. These what are ~~referred to as~~ value-added services give network operators the opportunity to differentiate themselves from competitors and to develop additional income sources.

In order to be able to offer value-added services, the network operator needs at least one central node in his network (service control point), which ^{stores} ~~has~~ the bits of information ~~stored~~ that are necessary for ^{eg.,} ~~purposes of~~ carrying out the services (storing the service programs, forwarding to responsible network nodes etc.). This central node is also referred to as implementing entity.

^{such} The users in a communication network can ~~thereby~~ utilize interesting new services.

One of the better known services is the ~~what is referred to as~~ ^{calling service, in which the} 'credit card calling'. The

caller is ~~hereby~~ charged via his credit card with the fees for actuated calls. Apart from

A Such an access protection is also imaginable regarding other services, for example for users in a mobile network, a private network or a private virtual network.

A In all these cases, the authenticating digit code is entered via the keyboard of the terminal device and is transparently (i.e., in plaintext) transmitted via the lines and switching nodes of the communication network.

A There are two possibilities to ^{inappropriately acquire} spy out these access codes:
 A a) by ^{acquiring} ~~spying out~~ the PIN, be it ^{by} observing the user ^{authorized} with respect to the input ^{entering it} via the keyboard of his terminal device, ^{or} also by video monitoring;
 A 10 b) by tapping the PIN with respect to the transmission between terminal device and the performing entity.

A SUMMARY OF THE INVENTION

The invention is based on the object of proposing a possibility as to how the access to services in a telecommunication network can be fashioned more secure.

INS A 10 This object is achieved by means of a method according to patent claim 1.

The utilized method describes the following course of action:

A 20 An ^{unambiguous} digit sequence for securing the access is encoded subsequent to ^{an} the input by ^{way} ~~means~~ of an encoding function or a mathematical one-way function, which are known to someone skilled in the art.

A A one-way function is a mathematical function $f(x) = y$, ^{in which} whereby y is simple to calculate; ^{from x; however} ~~vice versa~~, the determination of x from y , on the other hand, is extremely complex and not necessarily unambiguous.

A further parameter is co-encoded, which changes with each new input of the digit sequence. Therefore, each new encoding process supplies a new result.

3
result
A Together with the variable parameter, this is subsequently coded directly per protocol
A or is coded into a digit sequence, and is sent in multi-frequency signaling, potentially via
A switching nodes, up to the central entity.
The transmission ensues in the same way as the previous process of the
5 authentication.

Then, the central entity evaluates the transmitted digit sequence in that a result is also
A calculated from the known one-way function, using the expected PIN and the co-supplied
A parameters and is compared to the received value.
10

The realization of this authentication method is comparatively simple. A sufficient
number of encoding methods are known to someone skilled in the art. The
implementation of the method is only necessary on the side of the user and at the
A central entity; the implementation expenditure is low. An already-present data bank can be
A 15 simply expanded by a field for storing the already-received access codes.

The advantage of the described method clearly lies in the protection of the user. The
A expenditure outlay is not greater for the user than in previous methods, since an access code
A previously had to be entered as well. However, an unauthorized user is efficiently
20 prevented from calling at the expense of others. Misuse is they also required entry of
it is not a precondition that the user also has the credit card when he enters the credit
A card number, for example. Thus, the access could be gained in a simple way by means
A of simply observing the entered number including PIN.
A But with the inventive method
A In this case, the lacking knowledge about the utilized encoding method additionally
A 25 prevents from the unauthorized usage.

The access code is fashioned such that it is secure against tapping; one or more
variable parameters are added, such as a specification about the point in time of the

request. ~~Thereby, a tapping trial~~ in the network (for example on the access line) becomes useless, since a repeatedly used access code is rejected in the first place.

~~This object is achieved by means of a device according to patent claim 9.~~

5

A device for purposes of encoding the entered PIN is thereby utilized. This device requires an input device (keyboard) similar to the one of the communication terminal device. The device converts the entered digit sequence by means of the mathematical one-way function, together with a variable parameter. Together with the second parameter, the result of the calculation is subsequently translated into multi-frequency signaling methods and is transmitted to the terminal device.

The transmission up to the central entity ensues from there.

The central entity carries out an authentication with the received access code.

In addition to the previously cited advantages, a critical advantage of this course of ~~method/device~~ ^{digital sequence} ~~action~~ ^{long} is the possibility of being able to already enter the number a longer period of time before the actual usage. Thus, at least the 'spying-out' by means of observing the input of the number can be effectively prevented.

Advantageous embodiments and developments are provided in the subclaims.

The inventive course of action is particularly advantageous with respect to specific elements of telecommunication networks. First of all, the architecture of the intelligent network is to be specified, in which network, wherein, for example, the service 'credit card calling' has already been implemented. The infrastructure required for the method is already present in such a network. Apart from the private networks, which require a mechanism for accesses from outside, there is also the VPN - the 'Virtual Private Network', which is realized in IN technology as well. Finally, the method is also usable in communication

networks for mobile radio telephone service; ^{in these} here, the user must authenticate himself for a device as well.

A plurality of possibilities are imaginable for the variable parameters. In the most simple case, a random number is created each time; corresponding generator functions for random numbers are known to someone skilled in the art.

Another possibility is a time specification, for example, a dividing in a time-slot pattern of arbitrary nature. ^{an} ~~In this case~~ ^{in which}, the central entity, ~~on one hand~~ ^{furthermore}, can check whether the received access code is a current value. ~~Further~~ ^{further}, the additional transmission of the variable parameter is potentially not necessary when the transmitter and the receiver are ~~synchronized otherwise~~ ^{otherwise synchronized} in terms of time.

Another possibility is the generation of a mathematical progression with an initial number n , ^{in which} whereby the sequence number n_2 can result from its precursor number n_1 in different ways, such as summing ~~up~~ ^{values} a fixed ~~value~~ ^{value}.

Numerous methods and functions are known to someone skilled in the art regarding the type of encoding. In particular, the ITU recommendation X.509 and the RFC 1938 ^{are} represent different complex and secure authentication and encoding methods.

The ITU recommendation X.509 particularly represents two methods.

The first and more simple method only uses an encoding process. The one-way function f is applied to one or more variable parameters and the PIN, possibly expanded by a string that is known to the ^{Multi-Frequency (MFV)} ~~MFV~~ transmitter and the telecommunication service. The result from $f(\text{parameter1}, [\text{parameter2}, \dots], \text{PIN})$ is converted into a digit string, which is then transmitted by ^{way} ~~means~~ of the MFV transmitter.

It is more complex to realize a two-step encoding ^{which} ~~and it~~ also requires more computing power with respect to the transmitter and receiver; however, ^{two step encoding} it also offers a significantly higher protection.

In two step encoding, a

~~A~~ first encoding step ^{occurs} thereby ^{occurs} ensures in the same way as the above cited, single-step method. Subsequently, a second pass with a second mathematical algorithm f' (which can be identical with the first function f); the result calculates as follows:

f' (parameter x_1 [,parameter x_2 , ...], f' (parameter y_1 [,parameter y_2], PIN), PIN.

5

A generalized encoding process requires the multiple application of one algorithm or of different algorithms, respectively with the input parameters PIN and additional variable parameters.

10 When the result of the encoding is not a numeric digit sequence, or when the result cannot be transmitted without ^{MFV} ~~MFV~~ [sic] tones (as it is the case with respect to ISDN), the result must be translated in such a digit sequence prior to the transmission.

^{which determines}
The authentication method checks the transmitted digit code. ^{It is thereby detected}
^{determine}
15 whether the user is authorized to access a service. It can be additionally ~~detected~~
whether the digit code that is authorized to access a service is misused.

The authentication can proceed as follows:

- The central entity checks whether the sent access code has already been received once in a fixed time interval ^{and if so,}
- 20 ^{When this is the case} the authentication is discontinued as unsuccessful.
- ^{otherwise}
In the other case, the central entity calculates the access code to be expected by ^{way} ~~means~~ of the same one-way function and the second parameter contained in the received access code and compares the result to the
- 25 received one. The authentication is successful when the calculated and received code match. The user is allowed to access the desired service.

It can be advantageous to integrate the encoding device into the communication terminal device. ^{so that} ~~Thus~~, the user does not have a second device that can get lost.

Transmission errors of the encoding device to the terminal device are also avoided. A generator for MFV tones, which is already present in the terminal device, can be utilized and potentially modified.

- 5 The application possibilities of this method in a telecommunication network (particularly an intelligent network, a private network or a mobile network) are versatile. Particularly ^a the fee aspect represents a critical factor not only for the service provider but also for the network user.

- ^{Particularly}
A In particular, the credit card telephony is associated with an extremely high risk, ^{especially}
A 10 ^{Particularly} since the extent of the damage does not become obvious before the next invoice, since a loss of the card is not noticed in the case of misuse.

Both sides can achieve an extremely high advantage with a comparatively small expenditure ^{outlay}.

A BRIEF DESCRIPTION OF THE DRAWINGS

- 15 ^A The invention is subsequently explained on the basis of exemplary embodiments.

- A ~~Shown are~~ is a block diagram showing
A Figure 1 ^{the} generation, transmission and authentication of a one-time-access code in an intelligent network.
A Figure 2 ^{is a block diagram showing} the generation of the one-time-access code according to ^{the} ITU X.509, ^{single-step method, and}
20 ^{is a block diagram showing} the generation of the one-time-access code according to ^{the} ITU X.509, two-step method.
A Figure 3 ^{the}

A DESCRIPTION OF THE PREFERRED EMBODIMENTS

- ^{service control point}
A Figure 1 shows the path of an access key (PIN) from a user up to a central entity, ^A
25 (SCP) in an intelligent network.

Subsequent to the input in a device for purposes of encoding (MFV), the PIN is

- A transmitted ^{via} ~~by means~~ of dial tones to the terminal device (KE) and from there is
A transmitted into the communication network to the central entity (SCP). ~~En route,~~
INS A14 ~~switching centers (SSP) are passed via which the encoded access code is currently~~

INSAIS

A

A

A

A

A

10

A

15

20

A

f). 

Bibliography

ITU-T x.509

Information Technology - Open Systems Interconnection -

- 5 The Directory: Authentication Framework

ITU-T Recommendation x.509, 11/93

RFC 1938

Request for comments: 1938, May 1996

- 10 A one-time password system

N. Haller, Bellcore, C. Metz, Kaman Sciences Corporation

Abbreviation list

- | | | |
|----|-------|---------------------------------------|
| 15 | f, f | mathematical functions |
| | IN | intelligent network |
| | ITU | international telecommunication union |
| | KE | communication terminal device |
| | MFV | multi-frequency method |
| 20 | PIN | personal identification number |
| | rpPIN | replayprotected [sic]PIN |
| | SCP | service control point |
| | SSP | service switching point |